SIEMENS

PATENT
Attorney Docket No. 2002P15289WOUS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Inventor:	M. Franke et al.	)	Group Art Unit: 2434
		)	
Serial No.:	10/528,312	)	Examiner: Hailu, Teshome
		)	
Filed:	03/17/2005	)	Confirmation No.: 2692

Title: METHOD FOR GENERATING AND/OR VALIDATING ELECTRONIC SIGNATURES

Mail Stop Appeal Brief - Patent
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450
COMMISSIONER FOR PATENTS

APPELLANTS' REPLY BRIEF

Sir:

Pursuant to 37 C.F.R. § 41.41, this Reply Brief is responsive to the Examiner's Answer mailed 9 December 2009 in which the Examiner raised new substantive points of argument. This Reply Brief is not a substitute for the Appeal Brief. Any ground for rejection in the Examiner's Answer that is not refuted herein is considered by Appellant to have been sufficiently argued in the Appeal Brief, such that no further comment is needed herein. Arguments herein focus on errors and new arguments presented in the Examiner's answer.

(Please proceed to the following page.)

The following argument applies to independent claims 6 and 18, although language of claim 6 is used to demonstrate inconsistency and deficiency in the Examiner's Answer. The Examiner's Answer provides further commentary on the final rejection and points of argument which still fail to read the following two recitations of claim 6 on the Oka reference:

(1) calculating an electronic signature for an *electronic document* by means of the private signature key and by applying a predeterminable signature function; and

(2) performing a certification of the public validation key wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.

With regard to recitation (1), the argument of the Examiner's Answer (see at page 3, last paragraph), cites paragraph 9 at page 1 of the Oka reference. This paragraph 9 first describes (see lines 5 – 10) sending "a generated public key to a certificate authority" such that a certificate authority sends back a public key certificate. Paragraph 9 also states (see lines 10 – 14) that "**documents** or other desired data using the acquired public key ..." are encrypted "using the acquired public key ..." In this context Oka appears to be disclosing a sequence in which after a certificate sends a public key certificate to an end entity, the **documents** are encrypted. It is in this context that the rejection reads Appellants' *electronic document* on the **documents** which are encrypted. It should also be noted that such discussion of documents which are encrypted is in the background section of the Oka reference and this disclosure is not related to the discussion of Figure 22.

With regard to recitation (2), further argument in the Examiner's Answer (see page 4, first full paragraph), contends that paragraphs 193 – 203 and Fig. 22 of the Oka reference show an example where a signature is verified (step 8) before the certificate is issued. First, this is not the same signature referred to in paragraph [0009]. Second, the signature referred to in step 8 is verified when the certificate is issued and not beforehand. This inconsistency cannot be reconciled with the language of recitation (2). The cited paragraphs 193 – 203 and Fig. 22 do not describe or relate to the electronic documents which are encrypted per paragraph [0009] of the Oka reference. Rather, the cited paragraphs 193 – 203 and Fig. 22 concern:

(step 6) a signature execution;

(step 7) sending a signed public key certificate to CA server 321;

(step 8) confirming whether the signature is valid;

(step 9) if valid, sending the signed certificate to a registration authority;

(step 10) sending the signed certificate to from the registration authority to a requesting end entity 300.

These steps are described in paragraphs [0199] – [0203] of the Oka reference. Introductory paragraphs [0192] and [0193] further explain that these steps 6 - 10 and the steps 1 – 5 (see paragraphs [0194] – [0198]) are exemplary of an end entity outputting a public key request to a registration authority per Figure 22. There is no discussion or disclosure in any of the cited paragraphs 193 – 203 or Fig. 22 of an electronic document which is encrypted per paragraph [0009] of the Oka reference. Nor is there discussion of both: "calculating an electronic signature for an electronic document and, when validating, recognizing only those signatures generated at a time prior to the certification as valid.

The disclosure of Oka cannot anticipate claim 6 because step 8 of Oka does not refer to "a signature for an electronic document ..." Instead, step 8 refers to a signature on a certificate. Paragraph [0201] (Step 8) reads as follows:

"The CA server 321 retrieves a verification key from the verification key database to check whether the signature on the received public key certificate is valid."

In summary, argument in support of rejecting claims 6 and 18 under Section 102 makes no reference to

(1) calculating an electronic signature for an *electronic document* ...

or to

(2) validating... [wherein] **only** those signatures generated *at a time **prior** to the certification* of the public validation key are recognized as valid.

In this regard, the "Response to Argument" in the Examiner's Answer (beginning at the last line on page 5 and continuing on to page 6) states that step 8 (which confirms whether the signature is valid) occurs before step 9 (which sends the signed certificate to a registration authority if the signature is valid). This does nothing to support the rejection because the signature referred to in steps 8 and 9 is the signature for a certificate. The rejection cannot contend that the claim reads on Figure 22. Furthermore, as previously argued, the rejection disregards the word "only" in recitation (2) of claim 6. No argument is present with regard to the limitation "only".

Finally, to underscore the inconsistency it is also noted that Figure 22 simply does not disclose "*signatures generated* at a time **prior** to the certification" per recitation (2) of claim 6. That is, the signature described therein is generated (step 10 per paragraph [0225] of Oka) **during** the time period (and **not before** the time period) that the certification *of the public validation key [is] recognized as valid.* It is during the time period in which steps 1 – 10 are performed that the signature for the certificate of Oka is generated. The limitation in claim 6, i.e., "only", relates to "*signatures generated* at a time **prior** to the certification"

Lastly, for purposes of clarification, it is noted that, in Figure 22 of Oka, HSM1 (331) is a hardware security module (see paragraph [0017] which (per paragraph [0197] in step 7 performs signature execution. Thus, although step 7 uses the words "signed message" in Figure 22, step 8 makes clear that this is only the public key certificate having the signature thereon.

7C. CONCLUSIONS

Further argument has been presented to demonstrate that the rejections of claims 6 and 18 are deficient. The Examiner has argued rejections when claimed features are absent from the references and not suggested by the prior art. The Examiner has written argument "as though" cited text contains the claimed subject matter, but a plain reading of the cited prior art text clearly shows that the rejections are without basis. Accordingly, none of the rejections can be sustained.

For all of the above-argued reasons, all of the rejections should be overturned and the claims should be allowed.

Please grant any extensions of time required to enter this paper. Please charge any appropriate fees due in connection with this paper or credit any overpayments to Deposit Acct. No. 19-2179.

Respectfully submitted,

Dated: Jan. 27, 2010

By: Janet D. Hood

Janet D. Hood
Registration No. 61,142
(407) 736-4234

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830